Adjacency Graphs, Irreducible Polynomials and Cyclotomy

Ming Li and Dongdai Lin

State Key Laboratory of Information Security,
Institute of Information Engineering,
Chinese Academy of Sciences, Beijing 100093, China
E-mail: {liming,ddlin}@iie.ac.cn

Abstract

We consider the adjacency graphs of linear feedback shift registers (LFSRs) with reducible characteristic polynomials. Let $l(x)$ be a characteristic polynomial, and $l(x) = l_1(x)l_2(x)\cdots l_r(x)$ be a decomposition of $l(x)$ into co-prime factors. Firstly, we show a connection between the adjacency graph of FSR($l(x)$) and the association graphs of FSR($l_i(x)$), $1 \leq i \leq r$. By this connection, the problem of determining the adjacency graph of FSR($l(x)$) is decomposed to the problem of determining the association graphs of FSR($l_i(x)$), $1 \leq i \leq r$, which is much easier to handle. Then, we study the association graph of LFSRs with irreducible characteristic polynomials and give a relationship between these association graphs and the cyclotomic numbers over finite fields. At last, some applications are suggested.

Keywords: MSC(94A55), feedback shift register, adjacency graph, De Bruijn sequence, irreducible polynomial, cyclotomy.

1 Introduction

A De Bruijn sequence of order n is a binary sequence of period 2^n which contains all the binary n-tuples [2]. De Bruijn sequences have many applications in cryptography and modern communication systems [6]. It is well known that there are $2^{2^{n-1}-n}$ De Bruijn sequences of order n [2, 5]. Even though their size is very large, we can construct only a small fraction of them efficiently by now [1, 3–5, 11, 12, 20]. A classical method to construct De Bruijn sequences is to consider a feedback shift register (FSR) producing several cycles which are then joined together to form a full cycle. Such a method is called the cycle joining method proposed by Golomb [6]. For the application of this method, we need to know the distribution of the conjugate pairs in the cycles of the FSR, which is generally difficult to analyze.

The distribution of the conjugate pairs in the cycles of an FSR is defined to be the adjacency graph of this FSR [9]. Until now, only some special linear feedback shift registers (LFSRs) have been totally analyzed about their adjacency graphs, for example, the LFSRs with characteristic polynomials of the form $p(x)$, $(1+x)^m p(x)$, $(1+x^m)p(x)$ and $p_1(x)p_2(x)\cdots p_k(x)$, where $p(x)$ and

$p_i(x)$, $i = 1, 2, \ldots, k$, are primitive polynomial and m is a small positive integer [10,13–16,19]. Their adjacency graphs were determined and De Bruijn sequences were constructed from them. Recently, a progress was made in the LFSRs with primitive-like characteristic polynomials, i.e., the LFSRs with characteristic polynomials of the form $l(x)p(x)$, where $l(x)$ is a polynomial of small degree (< 30), and $p(x)$ is a primitive polynomial [17]. The authors there defined the concept of association graphs of LFSRs, and they showed how to convert the problem of determining the adjacency graph of FSR($l(x)p(x)$) to the problem of determining the association graph of FSR($l(x)$).

In this paper, we further analyse the relationship between the adjacency graphs and the association graphs of LFSRs. Let $l(x)$ be a characteristic polynomial and $l(x) = l_1(x)l_2(x)\cdots l_r(x)$ be a decomposition of $l(x)$ into co-prime factors. Firstly, by using the theory of LFSRs, we express the cycle structure of FSR($l(x)$) in terms of the cycle structure of FSR($l_i(x)$), $1 \leq i \leq r$. Then we decompose the problem of determining the adjacency graph of FSR($l(x)$) to the to the problem of determining the association graphs of FSR($l_i(x)$), $1 \leq i \leq r$. We show that, in the case of $\gcd(\mathrm{per}(l_1(x)), l_2(x), \ldots, l_r(x)) = 1$ the adjacency graph of FSR($l(x)$) is totally determined by the association graphs of FSR($l_i(x)$), $1 \leq i \leq r$, and in the case of $\gcd(\mathrm{per}(l_1(x)), l_2(x), \ldots, l_r(x)) \neq 1$, the adjacency graph of FSR($l(x)$) is related to the solutions of a set of equations. Since the concept of association graphs of LFSRs is of importance, we study the association graphs of LFSRs with irreducible characteristic polynomials, and give a connection between the association graphs and the cyclotomic numbers over finite fields. Finally, we suggest some applications of these results.

The remainder of this paper is organized as follows. In Section 2, we introduce some necessary preliminaries. In Section 3, the cycle structure of FSR($l(x)$) is analyzed. Section 4 gives a relationship between the adjacency graph of FSR($l(x)$) and the association graphs of FSR($l_i(x)$), $1 \leq i \leq r$. Section 5 considers the association graphs of LFSRs with irreducible characteristic polynomials. In Section 6, we present some applications. We make a conclusion on this paper in Section 7.

2 Preliminaries

2.1 Feedback Shift Registers

Let $\mathbb{F}_2 = \{0, 1\}$ be the binary finite field, and $\mathbb{F}_2^n$ be the nth-dimensional vector space over $\mathbb{F}_2$. An n-variable Boolean function $f(x_0, x_1, \ldots, x_{n-1})$ is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$.

An n-stage feedback shift register (FSR) consists of n binary storage cells and a feedback function F regulated by a single clock. The characteristic function of this FSR is defined to be $f = F + x_n$. The FSR with characteristic function f is denoted by FSR(f). At every clock pulse, the current state $(s_0, s_1, \ldots, s_{n-1})$ is updated by $(s_1, s_2, \ldots, s_{n-1}, F(s_0, s_1, \ldots, s_{n-1}))$ and the bit s_0 is outputted. The output sequences of FSR(f), denoted by $G(f)$, are the 2^n sequences $\mathbf{s} = s_0 s_1 \ldots$, satisfying $s_{t+n} = F(s_t, s_{t+1}, \ldots, s_{t+n-1})$, or equivalently $f(s_t, s_{t+1}, \ldots, s_{t+n}) = 0$, for any $t \geq 0$. It is shown by Golomb [6] that all sequences in $G(f)$ are periodic if and only if the characteristic function f is nonsingular, i.e., of the form $f = x_0 + f_0(x_1, \ldots, x_{n-1}) + x_n$. In the following discussion, all characteristic functions are assumed to be nonsingular.

We use $(s_0 s_1 \dots s_{p-1})$ to denote the periodic sequence $\mathbf{s} = s_0 s_1 \dots s_{p-1} \dots$ with period p. The period of $\mathbf{s}$ is denoted by $\mathrm{per}(\mathbf{s})$. We define the left shift operator L on periodic sequences by $L^i\mathbf{s} = (s_i s_{i+1} \dots s_{i-1})$, where the subscripts are taken modulo p. Two periodic sequences $\mathbf{s}_1$ and $\mathbf{s}_2$ are called shift-equivalent if there exists an integer r such that $\mathbf{s}_1 = L^r\mathbf{s}_2$. The set $G(f)$ are partitioned into equivalent classes $G(f) = [\mathbf{s}_1] \cup [\mathbf{s}_2] \cup \cdots \cup [\mathbf{s}_k]$ such that two sequences are in the same equivalent class if and only if they are shift equivalent. Each equivalent class is called a cycle of $\mathrm{FSR}(f)$, and the partition is called the cycle structure of $\mathrm{FSR}(f)$. A cycle $[(s_0, s_1, \dots, s_{p-1})]$ can also be represented using the state cycle form $[\mathbf{S}_0, \mathbf{S}_1, \dots, \mathbf{S}_{p-1}]$, where $\mathbf{S}_i = (s_i, s_{i+1}, \dots, s_{i+n-1})$ for $0 \le i \le p-1$, and the subscribes are taken modulo p. The state $\mathbf{S}_i$ is just the state of the FSR at the moment that the bit s_i is ready to be outputted.

An FSR is called a linear feedback shift register (LFSR) if its characteristic function f is linear [21]. For a linear Boolean function $f(x_0, x_1, \dots, x_n) = a_0x_0 + a_1x_1 + \cdots + a_nx_n$, we can associate it with a univariate polynomial $l(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{F}_2[x]$. Most of the time, we do not discriminate between linear Boolean functions and univariate polynomials. And for convenience, we sometimes use $\mathrm{FSR}(l(x))$ to denote the LFSR with characteristic function $f(x)$. For an n-stage FSR, the periods of its output sequences are no more than 2^n. If this value is attained, we call the sequences De Bruijn sequences, and call the FSR maximum length FSR. The unique cycle in a maximum-length FSR is called a full cycle. For an n-stage LFSR, the periods of its output sequences are no more than $2^n - 1$. If this value is attained, we call the sequences m-sequences, and call the FSR maximum length LFSR. It is known that, $\mathrm{FSR}(l(x))$ is a maximum length LFSR if and only if $l(x)$ is primitive, that is, the period of $l(x)$, denoted by $\mathrm{per}(l(x))$, is $2^n - 1$.

2.2 Adjacency Graphs and Cyclotomy

For a state $\mathbf{S} = (s_0, s_1, \dots, s_{n-1})$, its conjugate is defined to be the state $\widehat{\mathbf{S}} = (\overline{s}_0, s_1, \dots, s_{n-1})$, where $\overline{s}_0$ is the binary complement of s_0. Two cycles C_1 and C_2 are said to be adjacent if there exists a conjugate pair $(\mathbf{S}, \widehat{\mathbf{S}})$ such that the state $\mathbf{S}$ is on C_1 while its conjugate $\widehat{\mathbf{S}}$ is on C_2. Conjugate pairs can be used to join cycles. For two cycles C_1 and C_2 that share a conjugate pair $(\mathbf{S}, \widehat{\mathbf{S}})$, we can join the two cycles into one cycle by interchanging the successors of $\mathbf{S}$ and $\widehat{\mathbf{S}}$. This is the basic idea of the cycle joining method that proposed by Golomb [6]. For the application of the cycle joining method, we need to find out the location of conjugate pairs shared by cycles. This leads us to the definition of adjacency graph.

Definition 1. *[9, 18] For an FSR, its adjacency graph is an undirected graph where the vertexes correspond to the cycles in it, and there exists an edge labeled with an integer $m > 0$ between two vertexes if and only if the two vertexes share m conjugate pairs.*

For any FSR, its adjacency graph is a connected graph, that is, we can always join the cycles in this FSR into a full cycle. This fact follows from the statement in [5]: C is a full cycle if and only if the existence of state $\mathbf{S}$ on C also implies the existence of its conjugate $\widehat{\mathbf{S}}$ on C. Every maximal spanning tree of an adjacency graph corresponds to a maximum length FSR, since this represents

a choice of adjacencies that repeatedly join two cycles into one ending with exactly one cycle, i.e., a full cycle. Therefore, for a given FSR, the number of full cycles that we can get from it by using the cycle joining method, is equal to the number of maximum spanning trees of its adjacency graph.

Let $\mathbb{F}_{2^n}$ be the finite field of 2^n elements, and α be a primitive element in $\mathbb{F}_{2^n}$. The field $\mathbb{F}_{2^n}$ can be expressed as $\mathbb{F}_{2^n} = \{0, \alpha^0, \alpha^1, \ldots, \alpha^{2^n-2}\}$. Let $d \geq 1$ be a divisor of $2^n - 1$. The cyclotomic classes $C_0, C_1, \ldots, C_{d-1}$ of $\mathbb{F}_{2^n}$ are defined by $C_i = \{\alpha^{i+jd} \mid 0 \leq j \leq \frac{2^n-1}{d} - 1\}$ for $0 \leq i \leq d-1$. For two integers l and m with $0 \leq l, m \leq d-1$, the cyclotomic number $(l, m)_d$ over $\mathbb{F}_{2^n}$ is defined as the number of elements $x \in C_l$ such that $1 + x \in C_m$. It should be noted that, the cyclotomic number $(l, m)_d$ is not a fixed number for given l, m, d and n, but affected by the primitive element α, that is, different primitive elements may give different cyclotomic numbers. We refer the reader to [7, 14] for more details.

In the case that n is an even number, we have $3|2^n - 1$. The cyclotomic numbers of order 3 over $\mathbb{F}_{2^n}$ are fixed numbers (means that they are not affected by the primitive element α), and they are given in the following lemma.

Lemma 1. *[7, 8, 14] The cyclotomic numbers of order 3 over finite field $\mathbb{F}_{2^n}$ are given by $(0,0)_3 = A, (0,1)_3 = (1,0)_3 = (2,2)_3 = B, (0,2)_3 = (2,0)_3 = (1,1)_3 = C$ and $(1,2)_3 = (2,1)_3 = D$, where $A = \frac{2^n+(-2)^{\frac{n}{2}+1}-8}{9}$, $B = C = \frac{2^n+(-2)^{\frac{n}{2}}-2}{9}$, and $D = \frac{2^n+(-2)^{\frac{n}{2}+1}+1}{9}$.*

We refer the reader to [8] for the relationship between the adjacency graphs of LFSRs with irreducible characteristic polynomials and the cyclotomic numbers over finite fields.

2.3 Association Graphs

The concept of association graphs of LFSRs was proposed in [17] to deal with the adjacency graphs of LFSRs with primitive-like characteristic polynomials.

Let $\mathbf{a} = a_0, a_1, \ldots, a_i, \ldots$ and $\mathbf{b} = b_0, b_1, \ldots, b_i, \ldots$ be two sequences, and c be an element in $\mathbb{F}_2$. The sum of the two sequences $\mathbf{a} + \mathbf{b}$ and the scalar product $c \cdot \mathbf{a}$ are defined to be $\mathbf{a} + \mathbf{b} = a_0 + b_0, a_1 + b_1, \ldots, a_i + b_i, \ldots$, and $c \cdot \mathbf{a} = ca_0, ca_1, \ldots, ca_i, \ldots$. Let $l(x) \in \mathbb{F}_2[x]$ be a polynomial of degree n. Then there are 2^n sequences in the set $G(l(x))$. It is well known that, the set $G(l(x))$ is a vector space of dimension n over $\mathbb{F}_2$ when endowed with the two operations $+$ and $\cdot$ defined above. Let $\mathbf{u}$ be a sequence in $G(l(x))$. Because $< G(l(x)), + >$ is a group, the mapping from $G(l(x))$ to itself:

$$\gamma_{\mathbf{u}} : \mathbf{a} \mapsto \mathbf{u} + \mathbf{a}$$

is a bijection. We note that, the bijection $\gamma_{\mathbf{u}}$ is not necessarily preserve the shift equivalent property, that is, for two shift equivalent sequences $\mathbf{a}$ and $\mathbf{b}$, their images $\gamma_{\mathbf{u}}(\mathbf{a})$ and $\gamma_{\mathbf{u}}(\mathbf{b})$ may not be shift equivalent. Therefore, two sequences in a same cycle of $G(l(x))$ may be mapped into different cycles. This lead us to the following definition.

Definition 2. *[17] Let $\mathbf{u}$ be a sequence in $G(l(x))$, $[\mathbf{s}_1]$ and $[\mathbf{s}_2]$ be two cycles in $G(l)$. The association number of $[\mathbf{s}_1]$ and $[\mathbf{s}_2]$ with respect to $\mathbf{u}$ is defined by*

$$R_{\mathbf{u}}([\mathbf{s}_1], [\mathbf{s}_2]) = \left| \left\{ (i, j) \mid L^i \mathbf{s}_1 + L^j \mathbf{s}_2 = \mathbf{u}, \substack{0 \leq i \leq \mathrm{per}(\mathbf{s}_1)-1 \\ 0 \leq j \leq \mathrm{per}(\mathbf{s}_2)-1} \right\} \right|.$$

It is easy to see that, the association number $R_{\mathbf{u}}([\mathbf{s}_1],[\mathbf{s}_2])$ is exactly the number of sequences in $[\mathbf{s}_1]$ whose image under $\gamma_{\mathbf{u}}$ is located in the cycle $[\mathbf{s}_2]$. In another word, $R_{\mathbf{u}}([\mathbf{s}_1],[\mathbf{s}_2]) = |\{(\mathbf{a},\mathbf{b}) \mid \mathbf{a}+\mathbf{b}=\mathbf{u}, \mathbf{a}\in[\mathbf{s}_1], \mathbf{b}\in[\mathbf{s}_2]\}|$. We can use a graph to characterise these relations of the cycles in $G(l(x))$. It is obvious that, these relations are influenced by the sequence $\mathbf{u}$.

Definition 3. *[17] Let* $\mathbf{u}$ *be a sequence in* $G(l(x))$*. The association graph of* $\mathrm{FSR}(l(x))$ *with respect to* $\mathbf{u}$ *is an undirected graph, where the vertexes correspond to the cycles in* $G(l(x))$*, and there is an edge labeled with* $R_{\mathbf{u}}([\mathbf{s}_1],[\mathbf{s}_2])$ *between two vertices* $[\mathbf{s}_1]$ *and* $[\mathbf{s}_2]$*.*

3 The Direct Sum Decomposition of $G(l(x))$

Let $l(x)$ be a characteristic polynomial of degree n, and $l(x) = l_1(x)l_2(x)\cdots l_r(x)$ be a decomposition of $l(x)$ into co-prime factors, that is, $\gcd(l_1(x), l_2(x), \ldots, l_r(x)) = 1$. Let the degree of $l_i(x)$ be m_i for $1 \le i \le r$. Without lose of generality, we can assume $m_1 \le m_2 \le \cdots \le m_r$. By the theory of LFSRs, the vector space $G(l(x))$ has the direct sum decomposition:

$$G(l(x)) = G(l_1(x)) + G(l_2(x)) + \cdots + G(l_r(x)).$$

Every sequence in $G(l(x))$ can be uniquely written as a sum of r sequences in $G(l_1(x))$, $G(l_2(x))$, $\cdots$, $G(l_r(x))$ respectively. Let $\mathbf{e}$ be the sequence generated by $\mathrm{FSR}(l(x))$ with the initial state $(1,0,\ldots,0)$. By the above discussion, $\mathbf{e}$ can be uniquely written as $\mathbf{e} = \mathbf{e}_1 + \mathbf{e}_2 + \cdots + \mathbf{e}_r$, where $\mathbf{e}_i \in G(l_i(x))$ for $i = 1, 2, \ldots, r$. We say $\mathbf{e}_i$ is the representative of $G(l_i(x))$ determined by $l(x)$ for $i = 1, 2, \ldots, r$. We should note that, the representative of $G(l_i(x))$ relies on $l(x)$. Different $l(x)$ may result in different representatives.

Theorem 1. *With the above notations, the minimal polynomial of* $\mathbf{e}_i$ *is* $l_i(x)$ *for* $1 \le i \le r$*.*

Proof. It is obvious that, the minimal polynomial of $\mathbf{e}$ is $l(x)$. Suppose the minimal polynomial of $\mathbf{e}_i$ is not $l_i(x)$, but a proper divisor of $l_i(x)$. Then the minimal polynomial of the sum $\mathbf{e}_1+\mathbf{e}_2+\cdots+\mathbf{e}_r$ would be a proper divisor of $l(x)$, which is a contradiction. □

For a given $l(x)$ and a given decomposition $l(x) = l_1(x)l_2(x)\cdots l_r(x)$ satisfying $\gcd(l_1(x), l_2(x), \ldots, l_r(x)) = 1$, the representatives $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_r$ can be obtained by using Algorithm 1. In this algorithm, we use $\mathrm{FSR}(l(x), \mathbf{S})$ to denote the sequence generated by $\mathrm{FSR}(l(x))$ with initial state $\mathbf{S}$, and $\mathbf{U}|_k$ to denote the first k bits of the bit string $\mathbf{U}$. It is easy to see that, the time complicity of Algorithm 1 is $O(n2^{m_i})$. So, we can get the decomposition $\mathbf{e} = \mathbf{e}_1+\mathbf{e}_2+\cdots+\mathbf{e}_r$ in time $O(n(2^{m_1} + 2^{m_2} + \cdots + 2^{m_r}))$. In fact the time complicity can be optimized to $O(n(2^{m_1} + 2^{m_2} + \cdots + 2^{m_{r-1}}))$, because when the $r-1$ representatives $\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_{r-1}$ are obtained, the representative $\mathbf{e}_r$ can be determined by $\mathbf{e}_r = \mathbf{e} + \mathbf{e}_1 + \ldots + \mathbf{e}_{r-1}$.

In the following, we consider the cycle structure of $\mathrm{FSR}(l(x))$. For a periodic sequence $\mathbf{a}$, we use $[\mathbf{a}]$ to denote the cycle $[\mathbf{a}] = \{\mathbf{a}, L\mathbf{a}, \ldots, L^{\mathrm{per}(\mathbf{a})-1}\mathbf{a}\}$. The sum of two cycles $[\mathbf{a}]$ and $[\mathbf{b}]$ is defined to be $[\mathbf{a}] + [\mathbf{b}] = \{\mathbf{s}+\mathbf{t} \mid \mathbf{s}\in[\mathbf{a}], \mathbf{t}\in[\mathbf{b}]\}$. The following lemma was proved in [17].

Algorithm 1 Generation of the representative of $G(l_i(x))$

Input: The characteristic polynomial $l(x) = l_1(x)l_2(x)\cdots l_r(x)$.

Output: The representative of $G(l_i(x))$ determined by $l(x)$.

1: **for** $\mathbf{S} \in \mathbb{F}_2^{m_i}$ **do**
2: $\quad \mathbf{T} \leftarrow \mathrm{FSR}(l_i(x), \mathbf{S})|_n$
3: $\quad \mathbf{U} \leftarrow \mathbf{T} + (1, 0, \ldots, 0)$
4: $\quad \mathbf{U_0} \leftarrow \mathbf{U}|_{n-m_i}$
5: $\quad$ **if** $\mathbf{U} = \mathrm{FSR}(l(x)/l_i(x), \mathbf{U_0})|_n$ **then**
6: $\quad\quad \mathbf{u} \leftarrow \mathrm{FSR}(l_i(x), \mathbf{S})$
7: $\quad$ **end if**
8: **end for**
9: return $\mathbf{u}$

Lemma 2. *[17] Let* $\mathbf{s}_1$ *and* $\mathbf{s}_2$ *be two periodic sequences such that their minimal polynomials are co-prime. Let* $d = \gcd(\mathrm{per}(\mathbf{s}_1), \mathrm{per}(\mathbf{s}_2))$. *Then* $[\mathbf{s}_1] + [\mathbf{s}_2] = [\mathbf{s}_1 + \mathbf{s}_2] \cup [L\mathbf{s}_1 + \mathbf{s}_2] \cup \cdots \cup [L^{d-1}\mathbf{s}_1 + \mathbf{s}_2]$. *In particular, when* $\gcd(\mathrm{per}(\mathbf{s}_1), \mathrm{per}(\mathbf{s}_2)) = 1$, *we have* $[\mathbf{s}_1] + [\mathbf{s}_2] = [\mathbf{s}_1 + \mathbf{s}_2]$.

This lemma can be generalised to a more general case.

Lemma 3. *Let* $\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_r$ *be periodic sequences such that their minimal polynomials are co-prime. Let* $d_i = \gcd(\mathrm{per}(\mathbf{s}_1 + \cdots + \mathbf{s}_i), \mathrm{per}(\mathbf{s}_{i+1}))$ *for* $i = 1, 2, \ldots, r-1$. *Then we have,*

$$\begin{aligned}&[\mathbf{s}_1] + [\mathbf{s}_2] + \cdots + [\mathbf{s}_r]\\ &= \cup_{I_1=0}^{d_1-1} \cup_{I_2=0}^{d_2-1} \cdots \cup_{I_{r-1}=0}^{d_{r-1}-1} [L^{I_1+I_2+\cdots+I_{r-1}}\mathbf{s}_1 + L^{I_2+\cdots+I_{r-1}}\mathbf{s}_2 + \cdots + L^{I_{r-1}}\mathbf{s}_{r-1} + \mathbf{s}_r].\end{aligned}$$

In particular, when $\gcd(\mathrm{per}(\mathbf{s}_1), \mathrm{per}(\mathbf{s}_2), \ldots, \mathrm{per}(\mathbf{s}_r)) = 1$, *we have*

$$[\mathbf{s}_1] + [\mathbf{s}_2] + \cdots + [\mathbf{s}_r] = [\mathbf{s}_1 + \mathbf{s}_2 + \cdots + \mathbf{s}_r].$$

Proof.

$$\begin{aligned}&[\mathbf{s}_1] + [\mathbf{s}_2] + \cdots + [\mathbf{s}_r]\\ &= \left(\cup_{I_1=0}^{d_1-1}[L^{I_1}\mathbf{s}_1 + \mathbf{s}_2]\right) + [\mathbf{s}_3] + \cdots + [\mathbf{s}_r]\\ &= \left(\cup_{I_1=0}^{d_1-1} \cup_{I_2=0}^{d_2-1} [L^{I_1+I_2}\mathbf{s}_1 + L^{I_2}\mathbf{s}_2 + \mathbf{s}_3]\right) + [\mathbf{s}_4] + \cdots + [\mathbf{s}_r]\\ &\quad \cdots\\ &= \cup_{I_1=0}^{d_1-1} \cup_{I_2=0}^{d_2-1} \cdots \cup_{I_{r-1}=0}^{d_{r-1}-1} [L^{I_1+I_2+\cdots+I_{r-1}}\mathbf{s}_1 + L^{I_2+\cdots+I_{r-1}}\mathbf{s}_2 + \cdots + L^{I_{r-1}}\mathbf{s}_{r-1} + \mathbf{s}_r]\end{aligned}$$

□

By using this lemma, we can express the cycle structure of $G(l(x))$ in terms of the cycle structure of $G(l_i(x))$, $1 \le i \le r$.

Theorem 2. *Let $l(x)$ be a characteristic polynomial and $l(x) = l_1(x)l_2(x)\cdots l_r(x)$ be a decomposition of $l(x)$ into co-prime factors. Suppose the cycle structure of $G(l_1(x)), G(l_2(x)), \ldots, G(l_r(x))$ are*

$$\begin{aligned} G(l_1(x)) =& [\mathbf{s}_{1,1}] \cup [\mathbf{s}_{1,2}] \cup \cdots \cup [\mathbf{s}_{1,k_1}] \\ G(l_2(x)) =& [\mathbf{s}_{2,1}] \cup [\mathbf{s}_{2,2}] \cup \cdots \cup [\mathbf{s}_{2,k_2}] \\ & \vdots \\ G(l_r(x)) =& [\mathbf{s}_{r,1}] \cup [\mathbf{s}_{r,2}] \cup \cdots \cup [\mathbf{s}_{r,k_r}], \end{aligned}$$

where k_i is the number of cycles in $G(l_i(x))$ for $1 \le i \le r$. Then we have,

1. *In the case of* $\gcd(\mathrm{per}(l_1(x)), \mathrm{per}(l_2(x)), \ldots, \mathrm{per}(l_r(x))) = 1$, *the cycle structure of $G(l(x))$ is*

$$G(l(x)) = \cup_{i_1=1}^{k_1} \cup_{i_2=1}^{k_2} \cdots \cup_{i_r=1}^{k_r} [\mathbf{s}_{1,i_1} + \mathbf{s}_{2,i_2} + \cdots + \mathbf{s}_{r,i_r}].$$

2. *In the case of* $\gcd(\mathrm{per}(l_1(x)), \mathrm{per}(l_2(x)), \ldots, \mathrm{per}(l_r(x))) \neq 1$, *the cycle structure of $G(l(x))$ is*

$$\begin{aligned} G(l(x)) = & \left(\cup_{i_1=1}^{k_1} \cup_{i_2=1}^{k_2} \cdots \cup_{i_r=1}^{k_r}\right) \left(\cup_{I_1=0}^{d_1-1} \cup_{I_2=0}^{d_2-1} \cdots \cup_{I_{r-1}=0}^{d_{r-1}-1}\right) \\ & [L^{I_1+I_2\cdots+I_{r-1}}\mathbf{s}_{1,i_1} + L^{I_2\cdots+I_{r-1}}\mathbf{s}_{2,i_2} + \cdots + L^{I_{r-1}}\mathbf{s}_{r-1,i_{r-1}} + \mathbf{s}_{r,i_r}], \end{aligned}$$

where $d_j = \gcd(\mathrm{per}(\mathbf{s}_{1,i_1} + \cdots + \mathbf{s}_{j,i_j}), \mathrm{per}(\mathbf{s}_{j+1,i_{j+1}}))$ for $j = 1, 2, \ldots, r-1$.

Proof. It is easy to see that, Item 1 is a special case of Item 2. So for the proof of this theorem, we just need to show Item 2.

Because $l_1(x), l_2(x), \ldots, l_r(x)$ are co-prime polynomials, we have the direct sum decomposition $G(l(x)) = G(l_1(x)) + G(l_2(x)) + \cdots + G(l_r(x))$. Then Item 2 can be shown as follows,

$$\begin{aligned} G(l(x)) =& G(l_1(x)) + G(l_2(x)) + \cdots + G(l_r(x)) \\ =& \left(\cup_{i_1=1}^{l_1}[\mathbf{s}_{1,i_1}]\right) + \left(\cup_{i_2=1}^{l_2}[\mathbf{s}_{1,i_2}]\right) + \cdots + \left(\cup_{i_r=1}^{l_r}[\mathbf{s}_{1,i_r}]\right) \\ =& \left(\cup_{i_1=1}^{l_1} \cup_{i_2=1}^{l_2} \cdots \cup_{i_r=1}^{l_r}\right) ([\mathbf{s}_{1,i_1}] + [\mathbf{s}_{1,i_2}] + \cdots + [\mathbf{s}_{1,i_r}]) \\ =& \left(\cup_{i_1=1}^{l_1} \cup_{i_2=1}^{l_2} \cdots \cup_{i_r=1}^{l_r}\right) \left(\cup_{I_1=0}^{d_1-1} \cup_{I_2=0}^{d_2-1} \cdots \cup_{I_{r-1}=0}^{d_{r-1}-1}\right) \\ & [L^{I_1+I_2\cdots+I_{r-1}}\mathbf{s}_{1,i_1} + L^{I_2\cdots+I_{r-1}}\mathbf{s}_{2,i_2} + \cdots + L^{I_{r-1}}\mathbf{s}_{r-1,i_{r-1}} + \mathbf{s}_{r,i_r}] \end{aligned}$$

The last equation is valid because of Lemma 3. □

4 The Adjacency Graph of $\mathrm{FSR}(l(x))$

The cycle structure of $G(l(x))$ has been considered in Theorem 2. By the result there, in the case of $\gcd(\mathrm{per}(l_1(x)), \mathrm{per}(l_2(x)), \ldots, \mathrm{per}(l_r(x))) = 1$, the cycles in $G(l(x))$ has the form $[\mathbf{s}_1 + \mathbf{s}_2 + \cdots + \mathbf{s}_r]$, where $\mathbf{s}_i$ is a sequence in $G(l_i(x))$ for $i = 1, 2, \ldots, r$. In the case of $\gcd(\mathrm{per}(l_1(x)), \mathrm{per}(l_2(x)), \ldots,$

$\mathrm{per}(l_r(x))) \neq 1$, the cycles in $G(l(x))$ has the form $[L^{a_1}\mathbf{s}_1 + L^{a_2}\mathbf{s}_2 + \cdots + L^{a_r}\mathbf{s}_r]$, where $\mathbf{s}_i$ is a sequence in $G(l_i(x))$ and a_i is an integer satisfying $0 \leq a_i \leq \mathrm{per}(\mathbf{s}_i)$ for $1 \leq i \leq r$. Note that if $\gcd(\mathrm{per}(\mathbf{s}_1), \mathrm{per}(\mathbf{s}_1), \ldots, \mathrm{per}(\mathbf{s}_1)) \neq 1$, then different arrays $(a_1, a_2, \ldots, a_r) \neq (b_1, b_2, \ldots, b_r)$ may give the same cycle $[L^{a_1}\mathbf{s}_1 + L^{a_2}\mathbf{s}_2 + \cdots + L^{a_r}\mathbf{s}_r] = [L^{b_1}\mathbf{s}_1 + L^{b_2}\mathbf{s}_2 + \cdots + L^{b_r}\mathbf{s}_r]$. Theorem 2 can be used to depict when this happens, because it gives a full list of the cycles in $G(l(x))$ without repeating.

In this section, we consider the adjacency graph of $\mathrm{FSR}(l(x))$. We will give formulas for the number of conjugate pairs shared by cycles in $G(l(x))$. Our discussions are divided into two cases, the case of $\gcd(\mathrm{per}(l_1(x)), \mathrm{per}(l_2(x)), \ldots, \mathrm{per}(l_r(x))) = 1$ and the case of $\gcd(\mathrm{per}(l_1(x)), \mathrm{per}(l_2(x)), \ldots, \mathrm{per}(l_r(x))) \neq 1$.

Theorem 3. *In the case of* $\gcd(\mathrm{per}(l_1(x)), \mathrm{per}(l_2(x)), \ldots, \mathrm{per}(l_r(x))) = 1$, *let* $[\mathbf{s}_1 + \mathbf{s}_2 + \cdots + \mathbf{s}_r]$ *and* $[\mathbf{t}_1 + \mathbf{t}_2 + \cdots + \mathbf{t}_r]$ *be two cycles in* $G(l(x))$, *where* $\mathbf{s}_i$ *and* $\mathbf{t}_i$ *are two sequences in* $G(l_i(x))$ *for any* $1 \leq i \leq r$. *Then the number of conjugate pairs shared by the two cycles is*

$$\begin{aligned} &N([\mathbf{s}_1 + \mathbf{s}_2 + \cdots + \mathbf{s}_r], [\mathbf{t}_1 + \mathbf{t}_2 + \cdots + \mathbf{t}_r]) \\ =&R_{\mathbf{e}_1}([\mathbf{s}_1], [\mathbf{t}_1]) R_{\mathbf{e}_2}([\mathbf{s}_2], [\mathbf{t}_2]) \cdots R_{\mathbf{e}_r}([\mathbf{s}_r], [\mathbf{t}_r]). \end{aligned}$$

Proof. Write the cycles in the state form, where each state is of length m.

$$\begin{aligned} [\mathbf{s}_1] =&[\mathbf{S}_{1,0}, \mathbf{S}_{1,1}, \ldots, \mathbf{S}_{1,\mathrm{per}(\cdot)-1}] & [\mathbf{t}_1] =&[\mathbf{T}_{1,0}, \mathbf{T}_{1,1}, \ldots, \mathbf{T}_{1,\mathrm{per}(\cdot)-1}] \\ [\mathbf{s}_2] =&[\mathbf{S}_{2,0}, \mathbf{S}_{2,1}, \ldots, \mathbf{S}_{2,\mathrm{per}(\cdot)-1}] & [\mathbf{t}_2] =&[\mathbf{T}_{2,0}, \mathbf{T}_{2,1}, \ldots, \mathbf{T}_{2,\mathrm{per}(\cdot)-1}] \\ \vdots & & \vdots & \\ [\mathbf{s}_r] =&[\mathbf{S}_{r,0}, \mathbf{S}_{r,1}, \ldots, \mathbf{S}_{r,\mathrm{per}(\cdot)-1}] & [\mathbf{t}_r] =&[\mathbf{T}_{r,0}, \mathbf{T}_{r,1}, \ldots, \mathbf{T}_{r,\mathrm{per}(\cdot)-1}] \end{aligned}$$

For simplicity, we use the notation $\mathrm{per}(\cdot)$ to denote the period of the corresponding sequence. We need to show that, there is an one-to-one correspondence between the conjugate pairs shared by the two cycles $[\mathbf{s}_1 + \mathbf{s}_2 + \cdots + \mathbf{s}_r]$ and $[\mathbf{t}_1 + \mathbf{t}_2 + \cdots + \mathbf{t}_r]$ and the integer pairs $(u_1, v_1), (u_2, v_2), \ldots, (u_r, v_r)$ satisfying

$$L^{u_1}\mathbf{s}_1 + L^{v_1}\mathbf{t}_1 = \mathbf{e}_1, L^{u_2}\mathbf{s}_2 + L^{v_2}\mathbf{t}_2 = \mathbf{e}_2, \cdots, L^{u_r}\mathbf{s}_r + L^{v_r}\mathbf{t}_r = \mathbf{e}_r. \tag{1}$$

Suppose there exist pairs $(u_1, v_1), (u_2, v_2), \ldots, (u_r, v_r)$ satisfying Equation (1). Then we have

$$L^{u_1}\mathbf{s}_1 + L^{v_1}\mathbf{t}_1 + L^{u_2}\mathbf{s}_2 + L^{v_2}\mathbf{t}_2 + \cdots + L^{u_r}\mathbf{s}_r + L^{v_r}\mathbf{t}_r = \mathbf{e},$$

which implies

$$\mathbf{S}_{1,u_1} + \mathbf{T}_{1,v_1} + \mathbf{S}_{2,u_2} + \mathbf{T}_{2,v_2} + \cdots + \mathbf{S}_{r,u_r} + \mathbf{T}_{r,v_r} = \mathbf{E}, \tag{2}$$

where $\mathbf{E} = (1, 0, \ldots, 0)$. Define

$$\begin{aligned} \mathbf{X} &= \mathbf{S}_{1,u_1} + \mathbf{S}_{2,u_2} + \cdots + \mathbf{S}_{r,u_r} \\ \mathbf{Y} &= \mathbf{T}_{1,v_1} + \mathbf{T}_{2,v_2} + \cdots + \mathbf{T}_{r,v_r}. \end{aligned}$$

Equation (2) shows that, $(\mathbf{X}, \mathbf{Y})$ is a conjugate pair shared by the two cycles $[\mathbf{s}_1 + \mathbf{s}_2 + \cdots + \mathbf{s}_r]$ and $[\mathbf{t}_1 + \mathbf{t}_2 + \cdots + \mathbf{t}_r]$.

On the other hand, suppose $(\mathbf{X}, \mathbf{Y})$ is a conjugate pair shared by the two cycles $[\mathbf{s}_1 + \mathbf{s}_2 + \cdots + \mathbf{s}_r]$ and $[\mathbf{t}_1 + \mathbf{t}_2 + \cdots + \mathbf{t}_r]$. Since $\mathbf{X}$ is a state on the cycle $[\mathbf{s}_1 + \mathbf{s}_2 + \cdots + \mathbf{s}_r]$ and $\mathbf{Y}$ is a state on the cycle $[\mathbf{t}_1 + \mathbf{t}_2 + \cdots + \mathbf{t}_r]$, we can assume

$$\mathbf{X} = \mathbf{S}_{1,u_1} + \mathbf{S}_{2,u_2} + \cdots + \mathbf{S}_{r,u_r}$$
$$\mathbf{Y} = \mathbf{T}_{1,v_1} + \mathbf{T}_{2,v_2} + \cdots + \mathbf{T}_{r,v_r}.$$

Then by $\mathbf{X} + \mathbf{Y} = \mathbf{E}$ we get

$$\mathbf{S}_{1,u_1} + \mathbf{T}_{1,v_1} + \mathbf{S}_{2,u_2} + \mathbf{T}_{2,v_2} + \cdots + \mathbf{S}_{r,u_r} + \mathbf{T}_{r,v_r} = \mathbf{E}.$$

Let $\mathcal{T}$ be the next state operation corresponding to FSR(g). For any integer $t \geq 0$, we have

$$\mathcal{T}^t \left(\mathbf{S}_{1,u_1} + \mathbf{T}_{1,v_1} + \mathbf{S}_{2,u_2} + \mathbf{T}_{2,v_2} + \cdots + \mathbf{S}_{r,u_r} + \mathbf{T}_{r,v_r}\right) = \mathcal{T}^t \mathbf{E},$$

which implies

$$\mathcal{T}^t \mathbf{S}_{1,u_1} + \mathcal{T}^t \mathbf{T}_{1,v_1} + \mathcal{T}^t \mathbf{S}_{2,u_2} + \mathcal{T}^t \mathbf{T}_{2,v_2} + \cdots + \mathcal{T}^t \mathbf{S}_{r,u_r} + \mathcal{T}^t \mathbf{T}_{r,v_r} = \mathcal{T}^t \mathbf{E}.$$

Therefore, the following equation holds,

$$L^{u_1}\mathbf{s}_1 + L^{v_1}\mathbf{t}_1 + L^{u_2}\mathbf{s}_2 + L^{v_2}\mathbf{t}_2 + \cdots + L^{u_r}\mathbf{s}_r + L^{v_r}\mathbf{t}_r = \mathbf{e}.$$

Then by the uniqueness of the decomposition of $\mathbf{e}$, we get that

$$L^{u_1}\mathbf{s}_1 + L^{v_1}\mathbf{t}_1 = \mathbf{e}_1, L^{u_2}\mathbf{s}_2 + L^{v_2}\mathbf{t}_2 = \mathbf{e}_2, \cdots, L^{u_r}\mathbf{s}_r + L^{v_r}\mathbf{t}_r = \mathbf{e}_r.$$

So we get the integer pairs $(u_1, v_1), (u_2, v_2), \ldots, (u_r, v_r)$ which satisfy Equation (1). This completes the proof. □

According to the proof of Theorem 3, the conjugate pairs shared by the two cycles $[\mathbf{s}_1 + \mathbf{s}_2 + \cdots + \mathbf{s}_r]$ and $[\mathbf{t}_1 + \mathbf{t}_2 + \cdots + \mathbf{t}_r]$ are exactly those $(\mathbf{S}_{1,u_1} + \mathbf{S}_{2,u_2} + \cdots + \mathbf{S}_{r,u_r}, \mathbf{T}_{1,v_1} + \mathbf{T}_{2,v_2} + \cdots + \mathbf{T}_{r,v_r})$, where the array $(u_1, u_2, \ldots, u_r, v_1, v_2, \ldots, v_r)$ satisfies $L^{u_1}\mathbf{s}_1 + L^{v_1}\mathbf{t}_1 = \mathbf{e}_1, L^{u_2}\mathbf{s}_2 + L^{v_2}\mathbf{t}_2 = \mathbf{e}_2, \cdots, L^{u_r}\mathbf{s}_r + L^{v_r}\mathbf{t}_r = \mathbf{e}_r$. Hence, the problem of finding conjugate pairs shared by cycles in $G(l(x))$ is decomposed into the problems of finding the association relations between the cycles in $G(l_i(x))$ for $i = 1, 2, \ldots, r$, which are obviously easier to handle.

We note that, in Theorem 3, we didn't require the two cycles $[\mathbf{s}_1 + \mathbf{s}_2 + \cdots + \mathbf{s}_r]$ and $[\mathbf{t}_1 + \mathbf{t}_2 + \cdots + \mathbf{t}_r]$ are different. When the two cycles are the same one, we get that, there are $\frac{1}{2}R_{\mathbf{e}_1}([\mathbf{s}_1], [\mathbf{s}_1])R_{\mathbf{e}_2}([\mathbf{s}_2], [\mathbf{s}_2]) \cdots R_{\mathbf{e}_r}([\mathbf{s}_r], [\mathbf{s}_r])$ conjugate pairs in the cycle $[\mathbf{s}_1 + \mathbf{s}_2 + \cdots + \mathbf{s}_r]$. Therefore, Theorem 3 considers all the adjacency relations of the cycles in FSR$(l(x))$.

Theorem 4. *In the case of* $\gcd(\mathrm{per}(l_1(x)), \mathrm{per}(l_2(x)), \ldots, \mathrm{per}(l_r(x))) \neq 1$, *let* $[L^{a_1}\mathbf{s}_1 + L^{a_2}\mathbf{s}_2 + \cdots + L^{a_r}\mathbf{s}_r]$ *and* $[L^{b_1}\mathbf{t}_1 + L^{b_2}\mathbf{t}_2 + \cdots + L^{b_r}\mathbf{t}_r]$ *be two cycles in* $G(l(x))$, *where* $\mathbf{s}_i$ *and* $\mathbf{t}_i$ *are two sequences in* $G(f_i)$, *and* a_i *and* b_i *are two integers satisfying* $0 \leq a_i \leq \mathrm{per}(\mathbf{s}_i), 0 \leq b_i \leq \mathrm{per}(\mathbf{t}_i)$ *for any* $1 \leq i \leq r$. *Then the number of conjugate pairs shared by the two cycles is equal to the number of arrays* $(u_1, u_2, \ldots, u_r, v_1, v_2, \ldots, v_r)$ *that satisfy the following three conditions:*

1. $L^{u_i}\mathbf{s}_i + L^{v_i}\mathbf{t}_i = \mathbf{e}_i$ *for any* $1 \le i \le r$.

2. $\gcd(u_i, u_j)|(a_i - a_j), \gcd(v_i, v_j)|(b_i - b_j)$ *for any* $1 \le i \ne j \le r$.

3. $0 \le u_i \le \mathrm{per}(\mathbf{s}_i), 0 \le v_i \le \mathrm{per}(\mathbf{t}_i)$ *for any* $1 \le i \le r$.

Proof. Write the cycles $[\mathbf{s}_1], [\mathbf{s}_2], \ldots, [\mathbf{s}_r], [\mathbf{t}_1], [\mathbf{t}_2], \ldots, [\mathbf{t}_r]$ in the state form as in the proof of Theorem 3. We need to show that there is an one-to-one correspondence between the conjugate pairs shared by the two cycles $[L^{a_1}\mathbf{s}_1 + L^{a_2}\mathbf{s}_2 + \cdots + L^{a_r}\mathbf{s}_r]$ and $[L^{b_1}\mathbf{t}_1 + L^{b_2}\mathbf{t}_2 + \cdots + L^{b_r}\mathbf{t}_r]$ and the vectors $(u_1, u_2, \ldots, u_r, v_1, v_2, \ldots, v_r)$ that satisfy the three conditions.

Suppose there exists a vector $(u_1, u_2, \ldots, u_r, v_1, v_2, \ldots, v_r)$ that satisfy the three conditions. Since this vector satisfies Condition (1) we have,

$$L^{u_1}\mathbf{s}_1 + L^{v_1}\mathbf{t}_1 + L^{u_2}\mathbf{s}_2 + L^{v_2}\mathbf{t}_2 + \cdots + L^{u_r}\mathbf{s}_r + L^{v_r}\mathbf{t}_r = \mathbf{e}.$$

Let $\mathbf{X} = \mathbf{S}_{1,u_1} + \mathbf{S}_{2,u_2} + \cdots + \mathbf{S}_{r,u_r}$ and $\mathbf{Y} = \mathbf{T}_{1,v_1} + \mathbf{T}_{2,v_2} + \cdots + \mathbf{T}_{r,v_r}$ Then as we have done in the proof of Theorem 3, we can show that $(\mathbf{X}, \mathbf{Y})$ is a conjugate pair. Since the vector $(u_1, u_2, \ldots, u_r, v_1, v_2, \ldots, v_r)$ satisfies Condition 2, that is, $\gcd(u_i, u_j)|(a_i - a_j)$ for any $1 \le i \ne j \le r$, the reader can verify that $\mathbf{X}$ is a state on the cycle $[L^{a_1}\mathbf{s}_1 + L^{a_2}\mathbf{s}_2 + \cdots + L^{a_r}\mathbf{s}_r]$. Similarly, since $\gcd(v_i, v_j)|(b_i - b_j)$ for any $1 \le i \ne j \le r$, $\mathbf{Y}$ is a state on the cycle $[L^{b_1}\mathbf{t}_1 + L^{b_2}\mathbf{t}_2 + \cdots + L^{b_r}\mathbf{t}_r]$. Therefore, $(\mathbf{X}, \mathbf{Y})$ is a conjugate pair shared by the two cycles $[L^{a_1}\mathbf{s}_1 + L^{a_2}\mathbf{s}_2 + \cdots + L^{a_r}\mathbf{s}_r]$ and $[L^{b_1}\mathbf{t}_1 + L^{b_2}\mathbf{t}_2 + \cdots + L^{b_r}\mathbf{t}_r]$.

On the other hand, suppose $(\mathbf{X}, \mathbf{Y})$ is a conjugate pair shared by the two cycles $[L^{a_1}\mathbf{s}_1 + L^{a_2}\mathbf{s}_2 + \cdots + L^{a_r}\mathbf{s}_r]$ and $[L^{b_1}\mathbf{t}_1 + L^{b_2}\mathbf{t}_2 + \cdots + L^{b_r}\mathbf{t}_r]$. We can assume,

$$\mathbf{X} = \mathbf{S}_{1,u_1} + \mathbf{S}_{2,u_2} + \cdots + \mathbf{S}_{r,u_r}$$
$$\mathbf{Y} = \mathbf{T}_{1,v_1} + \mathbf{T}_{2,v_2} + \cdots + \mathbf{T}_{r,v_r}.$$

Since $\mathbf{X}$ is state on the cycle $[L^{a_1}\mathbf{s}_1 + L^{a_2}\mathbf{s}_2 + \cdots + L^{a_r}\mathbf{s}_r]$, the reader can verify that $\gcd(u_i, u_j)$ is a divisor of $a_i - a_j$ for any $1 \le i \ne j \le r$. Similarly, since $\mathbf{Y}$ is state on the cycle $[L^{a_1}\mathbf{s}_1 + L^{a_2}\mathbf{s}_2 + \cdots + L^{a_r}\mathbf{s}_r]$, we have that $\gcd(u_i, u_j)$ is a divisor of $a_i - a_j$ for any $1 \le i \ne j \le r$. Therefore, the vector $(u_1, u_2, \ldots, u_r, v_1, v_2, \ldots, v_r)$ satisfies Condition (2). Because $(\mathbf{X}, \mathbf{Y})$ is a conjugate pair, the equation $\mathbf{X} + \mathbf{Y} = \mathbf{E}$ holds. This implies,

$$\mathbf{S}_{1,u_1} + \mathbf{T}_{1,v_1} + \mathbf{S}_{2,u_2} + \mathbf{T}_{2,v_2} + \cdots + \mathbf{S}_{r,u_r} + \mathbf{T}_{r,v_r} = \mathbf{E}.$$

Then as in the proof of Theorem 3, we can show that,

$$L^{u_1}\mathbf{s}_1 + L^{v_1}\mathbf{t}_1 = \mathbf{e}_1, L^{u_2}\mathbf{s}_2 + L^{v_2}\mathbf{t}_2 = \mathbf{e}_2, \cdots, L^{u_r}\mathbf{s}_r + L^{v_r}\mathbf{t}_r = \mathbf{e}_r,$$

which means that the vector $(u_1, u_2, \ldots, u_r, v_1, v_2, \ldots, v_r)$ satisfies Condition (1). This completes the proof. □

According to the proof of Theorem 4, the conjugate pairs shared by the two cycles $[L^{a_1}\mathbf{s}_1 + L^{a_2}\mathbf{s}_2 + \cdots + L^{a_r}\mathbf{s}_r]$ and $[L^{b_1}\mathbf{t}_1 + L^{b_2}\mathbf{t}_2 + \cdots + L^{b_r}\mathbf{t}_r]$ are exactly those $(\mathbf{S}_{1,u_1} + \mathbf{S}_{2,u_2} + \cdots + \mathbf{S}_{r,u_r}, \mathbf{T}_{1,v_1} + \mathbf{T}_{2,v_2} + \cdots + \mathbf{T}_{r,v_r})$, where the array $(u_1, u_2, \ldots, u_r, v_1, v_2, \ldots, v_r)$ satisfies the three conditions.

We note that, in Theorem 4, we didn't require the two cycles $[L^{a_1}\mathbf{s}_1 + L^{a_2}\mathbf{s}_2 + \cdots + L^{a_r}\mathbf{s}_r]$ and $[L^{b_1}\mathbf{t}_1 + L^{b_2}\mathbf{t}_2 + \cdots + L^{b_r}\mathbf{t}_r]$ are different. When the two cycles are the same one, we get the number of conjugate pairs in the cycle $[L^{a_1}\mathbf{s}_1 + L^{a_2}\mathbf{s}_2 + \cdots + L^{a_r}\mathbf{s}_r]$. Therefore, Theorem 4 considers all the adjacency relations of the cycles in $\mathrm{FSR}(l(x))$.

5 Irreducible Polynomials and Cyclotomy

According to Theorems 3 and 4, the adjacency graph of $\mathrm{FSR}(l(x))$ relies totally on the association graphs of $\mathrm{FSR}(l_1(x)), \mathrm{FSR}(l_2(x)), \ldots, \mathrm{FSR}(l_r(x))$. So it is helpful to study the association graphs of LFSRs. In [17], some general properties about the association graphs have been given. In this section, we consider especially the association graphs of LFSRs with irreducible characteristic polynomials. We will show that, their association graphs are related to the cyclotomic numbers over finite fields.

Let $g(x)$ be a irreducible polynomial of degree m and period p. Let $q = \frac{2^m-1}{p}$. By the theory of LFSRs, $G(g(x))$ contains the zero cycle $[\mathbf{0}]$ and q cycles of length p. Denote the q non-zero cycles by $[\mathbf{s}_0], [\mathbf{s}_1], \ldots, [\mathbf{s}_{q-1}]$, where $\mathbf{s}_0, \mathbf{s}_2, \ldots, \mathbf{s}_{q-1}$ are non-zero sequences in $G(g(x))$ that in different cycles. Let β be a root of g. We can construct a finite field $\mathbb{F}_{2^m}$ with $g(x)$ as a defining polynomial. Let $\alpha \in \mathbb{F}_{2^m}$ be a primitive element satisfying $\alpha^q = \beta$, then $\mathbb{F}_{2^m} = \mathbb{F}_2(\alpha) = \{0, \alpha^0, \alpha^1, \ldots, \alpha^{2^m-2}\}$. It is well known that, for any sequence $\mathbf{a} \in G(g)$, there exists a unique $\gamma \in \mathbb{F}_{2^m}$ such that $\mathbf{a} = (a_i) = (\mathrm{Tr}(\gamma\beta^i))$, where the trace function Tr is from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ and a_i is the i-th element of $\mathbf{a}$. Define a mapping,

$$\begin{aligned} \phi : G(g) &\to \mathbb{F}_{2^m} \\ \mathbf{a} &\mapsto \gamma. \end{aligned}$$

Then ϕ is an one-to-one mapping and has the properties that, for any sequences $\mathbf{a}$ and $\mathbf{b}$ in $G(g)$, $\phi(L\mathbf{a}) = \phi(\mathbf{a})\beta, \phi(\mathbf{a} + \mathbf{b}) = \phi(\mathbf{a}) + \phi(\mathbf{b})$. Define the cyclotomic classes with respect to α

$$\begin{aligned} C_0 &= \{\beta^0, \beta^1, \ldots, \beta^{p-1}\} \\ C_1 &= \{\alpha\beta^0, \alpha\beta^1, \ldots, \alpha\beta^{p-1}\} \\ &\cdots \\ C_{q-1} &= \{\alpha^{q-1}\beta^0, \alpha^{q-1}\beta^1, \ldots, \alpha^{q-1}\beta^{p-1}\} \end{aligned}$$

The set $\mathbb{F}_{2^m} \setminus \{0\}$ is partitioned into disjoint classes, i.e., $\mathbb{F}_{2^m} \setminus \{0\} = C_1 \cup C_2 \cup \cdots \cup C_{q-1}$. The class C_i is the i-th cyclotomic class of $\mathbb{F}_{2^m}$ with respect to α. We note that, different primitive element α may result in different partitions of $\mathbb{F}_{2^n} \setminus \{0\}$. For a cycle $[\mathbf{s}_i]$ in $G(g)$, denote

$$\phi([\mathbf{s}_i]) = \{\phi(\mathbf{s}_i), \phi(L\mathbf{s}_i), \ldots, \phi(L^{p-1}\mathbf{s}_i)\}.$$

Then it is easy to see that, $\phi([\mathbf{s}_i])$ is a cyclotomic class. Different cycles in $G(g)$ give different cyclotomic classes. and there is an one-to-one correspondence between the cycles in $G(g)$ and the cyclotomic classes of $\mathbb{F}_{2^m}$. Without lose of generality, in the following we assume $\phi([\mathbf{s}_i]) = C_i$ for $0 \le i \le q-1$.

Theorem 5. *Let* $\mathbf{s}$ *be a sequence in* $G(g)$*, and let* $\phi(\mathbf{s}) = \alpha^a\beta^b$*, where* a *and* b *are two integers satisfying* $0 \le a \le q-1$ *and* $0 \le b \le p-1$*. Then the association number of* $[\mathbf{s}_i]$ *and* $[\mathbf{s}_j]$ *with respect to* $\mathbf{s}$ *is*

$$R_{\mathbf{s}}([\mathbf{s}_i], [\mathbf{s}_j]) = (i-a, j-a)_q,$$

where the two integers $i-a$ *and* $j-a$ *are reduced modulo* q*.*

Proof. Let γ be an element in $\mathbb{F}_{2^m}$. We use $\gamma + C_i$ to denote the set $\{\gamma + \delta \mid \delta \in C_i\}$, and γC_i to denote the set $\{\gamma\delta \mid \delta \in C_i\}$. We need to prove that $|(\alpha^a\beta^b + C_i) \cap C_j| = (i-a, j-a)_q$. This can be done as follows,

$$\begin{aligned}
&|(\alpha^a\beta^b + C_i) \cap C_j| \\
=&|\alpha^{-a}\beta^{-b}((\alpha^a\beta^b + C_i) \cap C_j)| \\
=&|\alpha^{-a}((\alpha^a + C_i) \cap C_j)| \\
=&|(1 + C_{i-a}) \cap C_{j-a})| \\
=&(i-a, j-a)_q.
\end{aligned}$$

□

6 Applications

6.1 Applications to the product of primitive polynomials

Let $p(x)$ be a primitive polynomial of degree n. Then $G(p(x))$ contains two cycles, $[\mathbf{0}]$ and $[\mathbf{s}]$, where $\mathbf{0}$ is the zero sequence, and $\mathbf{s}$ is an m-sequence in $G(p(x))$.

Theorem 6. *Let* $p(x)$ *be a primitive polynomial of degree* n*, and* $G(p(x)) = [\mathbf{0}] \cup [\mathbf{s}]$ *where* $\mathbf{s}$ *is an* m*-sequence in* $G(p(x))$*. The association numbers of the cycles in* $G(p(x))$ *with respect to any* m*-sequence* $\mathbf{u} \in G(p(x))$ *is*

$$R_{\mathbf{u}}([\mathbf{0}], [\mathbf{0}]) = 0, R_{\mathbf{u}}([\mathbf{0}], [\mathbf{s}]) = 1, R_{\mathbf{u}}([\mathbf{s}], [\mathbf{s}]) = 2^n - 2.$$

Proof. It is easy to see that, $R_{\mathbf{u}}([\mathbf{0}], [\mathbf{0}]) = 0$ and $R_{\mathbf{u}}([\mathbf{0}], [\mathbf{s}]) = 1$. In the following, we show that $R_{\mathbf{u}}([\mathbf{s}], [\mathbf{s}]) = 2^n - 2$. By the definition of association numbers, $R_{\mathbf{u}}([\mathbf{s}], [\mathbf{s}]) = |\{\mathbf{s}_1 \mid \mathbf{u} + \mathbf{s}_1 \in [\mathbf{s}], \mathbf{s}_1 \in [\mathbf{s}]\}| = |G(p(x)) \setminus \{\mathbf{0}, \mathbf{u}\}| = 2^n - 2$. □

The association graphs of LFSRs is assumed to be obtained by using the exhaustive search method, that is, for a given polynomial $l(x)$ of degree m and a sequence $\mathbf{u} \in G(l(x))$, we need time $O(2^m)$ to calculate the association graph of FSR($l(x)$) with respect to $\mathbf{u}$. However, when

$l(x)$ is a primitive polynomial, by Theorem 6 the association graph of FSR($l(x)$) can be derived directly. We should note that, Theorem 3 together with Theorem 6 give the adjacency graph of $G(p_1(x)p_2(x)\cdots p_r(x))$, where $p_1(x), p_2(x), \ldots, p_r(x)$ are primitive polynomials such that $\gcd(\deg p_1(x), \deg p_1(x), \ldots, \deg p_1(x)) = 1$. These adjacency graphs have been studied in [15] using a different method. It is easy to verify that, $\gcd(\deg p_1(x), \deg p_1(x), \ldots, \deg p_1(x)) = 1$ if and only if $\gcd(\mathrm{per}(p_1(x)), \mathrm{per}(p_2(x)), \ldots, \mathrm{per}(p_r(x))) = 1$. By Theorem 2, when $\gcd(\deg p_1(x), \deg p_1(x), \ldots, \deg p_1(x)) = 1$ the cycles in $G(p_1(x)p_2(x)\cdots p_r(x))$ has the form $[\mathbf{s}_1 + \mathbf{s}_2 + \cdots + \mathbf{s}_r]$, where $\mathbf{s}_i$ is a sequence in $G(p_i)$.

Corollary 1. *[15] Let $p_1(x), p_2(x), \ldots, p_r(x)$ be primitive polynomials of degrees $n_1, n_2, \ldots, n_r$ respectively. Suppose $\gcd(n_1, n_2, \ldots, n_r) = 1$. Let $[\mathbf{s}_1 + \mathbf{s}_2 + \cdots + \mathbf{s}_r]$ and $[\mathbf{t}_1 + \mathbf{t}_2 + \cdots + \mathbf{t}_r]$ be two cycles in $G(p_1(x)p_2(x)\cdots p_r(x))$, where $\mathbf{s}_i$ and $\mathbf{t}_i$ are two sequences in $G(p_i(x))$ for $1 \le i \le r$. Then the number of conjugate pairs shared by the two cycles $[\mathbf{s}_1 + \mathbf{s}_2 + \cdots + \mathbf{s}_r]$ and $[\mathbf{t}_1 + \mathbf{t}_2 + \cdots + \mathbf{t}_r]$ is*

$$
\begin{aligned}
&N([\mathbf{s}_1 + \mathbf{s}_2 + \cdots + \mathbf{s}_r], [\mathbf{t}_1 + \mathbf{t}_2 + \cdots + \mathbf{t}_r]) \\
&= \left(\prod_{\mathbf{s}_i \neq \mathbf{0}, \mathbf{t}_i \neq \mathbf{0}} (2^{n_i} - 2) \right) \left(\prod_{\mathbf{s}_i = \mathbf{0}, \mathbf{t}_i \neq \mathbf{0}} 1 \right) \left(\prod_{\mathbf{s}_i \neq \mathbf{0}, \mathbf{t}_i = \mathbf{0}} 1 \right) \left(\prod_{\mathbf{s}_i = \mathbf{0}, \mathbf{t}_i = \mathbf{0}} 0 \right).
\end{aligned}
$$

Proof. Let $\mathbf{e}$ be the sequence generated by FSR($p_1(x)p_2(x)\cdots p_r(x)$) with the initial state (1, 0, ..., 0). The sequence $\mathbf{e}$ has the unique decomposition $\mathbf{e} = \mathbf{e}_1 + \mathbf{e}_2 + \cdots + \mathbf{e}_r$ such that $\mathbf{e}_r \in G(p_i(x))$ for $1 \le i \le r$. By Theorem 1, the minimal polynomial of $\mathbf{e}_i$ is $p_i(x)$, that is , $\mathbf{e}_i \neq \mathbf{0}$ for $1 \le i \le r$. By Theorem 3, $N([\mathbf{s}_1 + \mathbf{s}_2 + \cdots + \mathbf{s}_r], [\mathbf{t}_1 + \mathbf{t}_2 + \cdots + \mathbf{t}_r]) = R_{\mathbf{e}_1}([\mathbf{s}_1], [\mathbf{t}_1]) R_{\mathbf{e}_2}([\mathbf{s}_2], [\mathbf{t}_2]) \cdots R_{\mathbf{e}_r}([\mathbf{s}_r], [\mathbf{t}_r])$. Then we can finish the proof by using the formulas in Theorem 6. □

6.2 Applications to primitive-like polynomials

The primitive-like polynomials are of the form $l(x)p(x)$, where $l(x)$ be a polynomial of small degree and $p(x)$ be a primitive polynomial. Let $\deg l(x) = m$ and $\deg p(x) = n$. For simplicity, we consider here only the case of $\gcd(\mathrm{per}(l(x)), \mathrm{per}(p(x))) = 1$. Let $\mathbf{e}$ be the sequence generated by FSR($l(x)p(x)$) with the initial state $(1, 0, \ldots, 0)$, and $\mathbf{e} = \mathbf{u} + \mathbf{s}$ be the decomposition of $\mathbf{e}$ such that $\mathbf{u} \in G(l(x))$ and $\mathbf{s} \in G(p(x))$. It was shown in [15] that, the adjacency graph of FSR($l(x)p(x)$) is related to the association graph of FSR($l(x)$) with respect to $\mathbf{u}$. The decomposition $\mathbf{e} = \mathbf{u} + \mathbf{s}$ is assumed to be obtained in time $O(n2^m)$ and the association graph of FSR($l(x)$) is assumed to be obtained in time $O(2^m)$. Therefore, determining the adjacency graph of FSR($l(x)p(x)$) needs time $O(n2^m)$. In fact, the time complicity can be optimized as follows.

Let $l(x) = l_1(x)l_2(x)\cdots l_r(x)$ be a decomposition of $l(x)$ into co-prime factors. Let the degree of $l_i(x)$ be m_i for $1 \le i \le r$. Without lose of generality, we assume $m_1 \le m_2 \le \cdots \le m_r$. Let $\mathbf{e} = \mathbf{e_1} + \mathbf{e_2} + \cdots + \mathbf{e_r} + \mathbf{s}$ be the decomposition of $\mathbf{e}$ such that $\mathbf{e}_i \in G(l_i(x))$ for $1 \le i \le r$ and $\mathbf{s} \in G(p(x))$. It is easy to show that, $\mathbf{e_1} + \mathbf{e_2} + \cdots + \mathbf{e_r} = \mathbf{u}$. By using Algorithm 1, this decomposition can be obtained in time $O(n(2^{m_1} + 2^{m_2} + \cdots + 2^{m_r}))$. Then, by Theorem 3 we can get the adjacency graph of FSR($l(x)p(x)$) by analyzing the association graphs of FSR($l_i(x)$) with

respect to $\mathbf{e}_i$ for $1 \leq i \leq r$, which needs time $O(2^{m_1} + 2^{m_2} + \cdots + 2^{m_r})$. Therefore, the total time to determine the adjacency graph of FSR$(l(x)p(x))$ is $O(n(2^{m_1} + 2^{m_2} + \cdots + 2^{m_r}))$, which can be much smaller than $O(n2^m)$.

We use an example to explain the above discussion. The adjacency graph of FSR$((1+x+x^3+x^4)p(x))$ was analyzed in [17]. Since $1 + x + x^3 + x^4 = (1 + x^2)(1 + x + x^2)$, instead of analyzing the association graph of FSR$(1 + x + x^3 + x^4)$ with respect to $\mathbf{u} = (000111)$ (see Figures 1 and 2 in [17]), we can analyze the association graphs of FSR$(1 + x^2)$ and FSR$(1 + x + x^2)$ with respect to $\mathbf{e}_1 = (10)$ and $\mathbf{e}_2 = (101)$ respectively. The two mappings $\gamma_{\mathbf{e}_1}$ and $\gamma_{\mathbf{e}_2}$ are shown in Figures 1 and 2. The association graphs of FSR$(1 + x^2)$ and FSR$(1 + x + x^2)$ with respect to $\mathbf{e}_1 = (10)$ and $\mathbf{e}_2 = (101)$ respectively can be easily determined from two mappings $\gamma_{\mathbf{e}_1}$ and $\gamma_{\mathbf{e}_2}$, and they will not be given here.

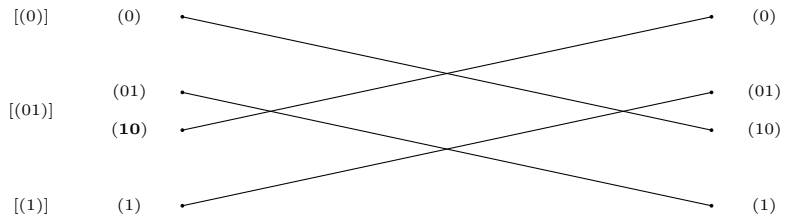

Figure 1: The mapping $\gamma_{\mathbf{e}_1}$ on $G(1 + x^2)$, where $\mathbf{e}_1 = (10)$

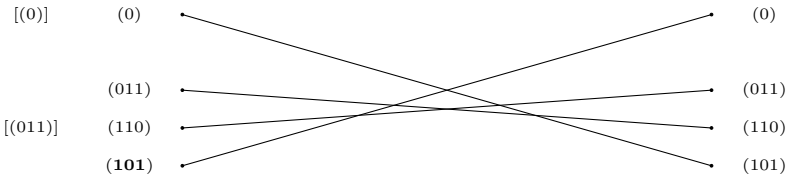

Figure 2: The mapping $\gamma_{\mathbf{e}_2}$ on $G(1 + x + x^2)$, where $\mathbf{e}_2 = (101)$

Let $\mathbf{s}$ be an m-sequence in $G(p(x))$. The cycle structure of $G(1+x^2)$, $G(1+x+x^2)$ and $G(p(x))$ are

$$G(1 + x^2) = [(0)] \cup [(01)] \cup [(1)]$$
$$G(1 + x + x^2) = [(0)] \cup [(011)]$$
$$G(p(x)) = [(0)] \cup [\mathbf{s}].$$

By Theorem 2, the cycle structure of FSR$((1+x^2)(1+x+x^2)p(x))$ is

$$\begin{aligned}
&G((1+x^2)(1+x+x^2)p(x))\\
=&[(0)+(0)+(0)]\cup[(01)+(0)+(0)]\cup[(1)+(0)+(0)]\\
&+[(0)+(011)+(0)]\cup[(01)+(011)+(0)]\cup[(1)+(011)+(0)]\\
&+[(0)+(0)+\mathbf{s}]\cup[(01)+(0)+\mathbf{s}]\cup[(1)+(0)+\mathbf{s}]\\
&+[(0)+(011)+\mathbf{s}]\cup[(01)+(011)+\mathbf{s}]\cup[(1)+(011)+\mathbf{s}]\\
=&[(0)]\cup[(01)]\cup[(1)]+[(011)]\cup[(000111)]\cup[(001)]\\
&+[\mathbf{s}]\cup[(01)+\mathbf{s}]\cup[(1)+\mathbf{s}]+[(011)+\mathbf{s}]\cup[(000111)+\mathbf{s}]\cup[(001)+\mathbf{s}].
\end{aligned}$$

From the association graphs of FSR$(1+x^2)$, FSR$(1+x+x^2)$ and FSR$(p(x))$, the adjacency graph of FSR$((1+x+x^2)(1+x^2)p(x))$ can be determined. We take the two cycles $[(011)]$ and $[(000111)+\mathbf{s}]$ for example to show how to calculate the number of conjugate pairs shared by them. Because $[(011)]=[(0)+(011)+(0)]$ and $[(000111)+\mathbf{s}]=[(01)+(011)+\mathbf{s}]$, by Theorem 3 the number of conjugate pairs shared by the two cycles is

$$N([(011)],[(000111)+\mathbf{s}])=R_{\mathbf{e}_1}([(0)],[(01)])R_{\mathbf{e}_2}([(011)],[(011)])R_{\mathbf{s}}([(0)],[\mathbf{s}])=2.$$

6.3 Applications to irreducible-like polynomials

We call the polynomials of the form $l(x)g(x)$ irreducible-like polynomials, where $l(x)$ is a polynomial of small degree and $g(x)$ is an irreducible polynomial. For simplicity, we consider here only the case of $\gcd(\mathrm{per}(l(x)),\mathrm{per}(g(x)))=1$. Let $\deg l(x)=m$ and $\deg g(x)=n$. Suppose $l(x)=l_1(x)l_2(x)\cdots l_r(x)$ is a decomposition of $l(x)$ into co-prime factors. Let the degree of $l_i(x)$ be m_i for $1\le i\le r$. Without lose of generality, we assume $m_1\le m_2\le\cdots\le m_r$. Let $\mathbf{e}$ be the sequence generated by FSR$(l(x)g(x))$ with the initial state $(1,0,\ldots,0)$, and $\mathbf{e}=\mathbf{e_1}+\mathbf{e_2}+\cdots+\mathbf{e_r}+\mathbf{s}$ be the decomposition of $\mathbf{e}$ such that $\mathbf{e}_i\in G(l_i(x))$ for $1\le i\le r$ and $\mathbf{s}\in G(g(x))$. By using Algorithm 1, this decomposition can be obtained in time $O(n(2^{m_1}+2^{m_2}+\cdots+2^{m_r}))$.

According to Theorem 3, to determine the adjacency graph of FSR$(l(x)g(x))$ we need to analyze the association graphs of FSR$(l_i(x))$ with respect to $\mathbf{e}_i$ for $1\le i\le r$ and the association graph of FSR$(g(x))$ with respect to $\mathbf{s}$. The association graphs of FSR$(l_i(x))$ for $1\le i\le r$ can be determined in time $O(2^{m_1}+2^{m_2}+\cdots+2^{m_r})$. The association graph of FSR$(g(x))$ with respect to $\mathbf{s}$ is related to the cyclotomic numbers over finite fields by Theorem 5. Let $\mathrm{per}(g(x))=p$ and $q=\frac{2^n-1}{p}$. Then $G(g(x))$ contains the zero cycle $[\mathbf{0}]$ and q nonzero cycles of length p. Denote the cycle structure by $G(g(x))=[\mathbf{0}]\cup[\mathbf{s}_0]\cup[\mathbf{s}_1]\cup\cdots\cup[\mathbf{s}_{q-1}]$, where $\mathbf{s}_1,\mathbf{s}_2,\ldots,\mathbf{s}_{q-1}$ are sequences in $G(g(x))$. Let β be a root of $g(x)$ and $\alpha\in\mathbb{F}_{2^n}$ be a primitive element satisfying $\alpha^q=\beta$, where $q=\frac{2^n-1}{p}$ and p is the period of $g(x)$. Without lose of generality, we assume $[\mathbf{s}_i]$ is the cycle that corresponding to the cyclotomic class $C_i=\{\alpha^i\beta^0,\alpha^i\beta^1,\ldots,\alpha^i\beta^{p-1}\}$ for $0\le i\le q-1$ (see the discussion in Section 5).

To determine the association graph of FSR$(g(x))$ with respect to $\mathbf{s}$, we have to know (1) which cycle $[\mathbf{s}_i]$ contains the sequence $\mathbf{s}$, and (2) the exact values of the related cyclotomic numbers. Question (1) can be related to the following problem (see Problem 1). It appears to us, however,

difficult to solve Problem 1 in time $O(n)$. The known methods to this problem need time that grow exponentially with n. For Question (2), only a few cyclotomic numbers are known by now (see Lemma 1). So it seems hard to determine the adjacency graph of LFSRs with irreducible-like characteristic polynomials in the general case.

Problem 1. *Let $g(x)$ be an irreducible polynomial of degree n, and $\mathbf{X}$ and $\mathbf{Y}$ be two states of length n. Determine whether or not the two states $\mathbf{X}$ and $\mathbf{Y}$ belong to the same cycle of $G(g(x))$.*

In the following, we consider the case of $\mathrm{per}(g(x)) = 3$ and $l(x) = 1 + x + x^2$ to show how to determine the adjacency graph of $\mathrm{FSR}(l(x)g(x))$. The two cycle structure of $G(l(x))$ and $G(g(x))$ are $G(l(x)) = [(0)] \cup [(011)]$ and $G(g(x)) = [(0)] \cup [\mathbf{s}_1] \cup [\mathbf{s}_2] \cup [\mathbf{s}_3]$, where $[\mathbf{s}_i]$ is the cycle that corresponding to the cyclotomic class $C_i = \{\alpha^i\beta^0, \alpha^i\beta^1, \ldots, \alpha^i\beta^{p-1}\}$ for $0 \le i \le 2$. By using Algorithm 1, we can get the decomposition $\mathbf{e} = \mathbf{e}_1 + \mathbf{s}$ in time $O(n)$, where $\mathbf{e}_1 \in G(l(x))$ and $\mathbf{s} \in G(g(x))$. We assume that the sequence $\mathbf{s}$ belongs to the cycle $[\mathbf{s}_0]$. The other cases can be handled similarly. Then the association graph of $\mathrm{FSR}(g(x))$ with respect to $\mathbf{s}$ can be determined by using Theorem 5, and we show it in Figure 3.

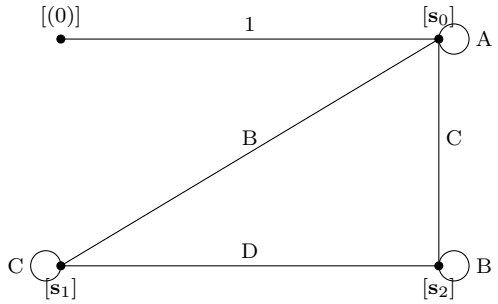

Figure 3: The association graph of $\mathrm{FSR}(g)$ with respect to $\mathbf{s}$

Then by using Theorem 3, we can get the adjacency graph of $\mathrm{FSR}((1 + x + x^2)g(x))$, and we show it in Figure 4. The number of conjugate pairs shared by cycles are listed in Table 1. The numbers A,B,C and D are from Lemma 1. We should note that, these results are based on the assumption $\mathbf{s} \in [\mathbf{s}_0]$.

Table 1: The number of conjugate pairs shared by cycles in $\mathrm{FSR}((1 + x + x^2)g(x))$

	$[(0)]$	$[\mathbf{u}_0]$	$[\mathbf{u}_1]$	$[\mathbf{u}_2]$	$[(011)]$	$[(011) + \mathbf{u}_0]$	$[(011) + \mathbf{u}_1]$	$[(011) + \mathbf{u}_2]$
$[(0)]$	0	0	0	0	0	1	0	0
$[\mathbf{u}_0]$	0	0	0	0	1	A	B	C
$[\mathbf{u}_1]$	0	0	0	0	0	B	C	D
$[\mathbf{u}_2]$	0	0	0	0	0	C	D	B
$[(011)]$	0	1	0	0	0	2	0	0
$[(011) + \mathbf{u}_0]$	1	A	B	C	2	2A	2B	2C
$[(011) + \mathbf{u}_1]$	0	B	C	D	0	2B	2C	2D
$[(011) + \mathbf{u}_2]$	0	C	D	B	0	2C	2D	2B

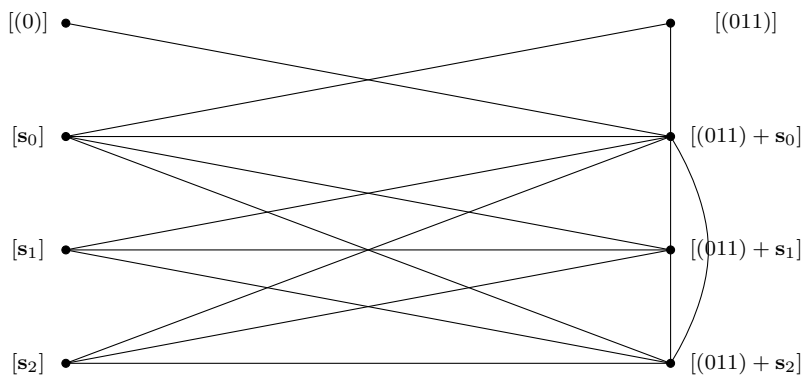

Figure 4: The adjacency graph of FSR$((1+x+x^2)g(x))$

7 Conclusion

We studied the relationship between the adjacency graphs and the association graphs of LFSRs. By using this relationship, the problem of determining the adjacency graphs of LFSRs is decomposed to the problem of determining the association graphs of LFSRs with small orders, which is much easier to handle. We also studied the association graphs of LFSRs with irreducible characteristic polynomials, and showed that these association graphs are related to the cyclotomic numbers over finite fields. At the end, we suggested some applications of these results.

References

[1] F. S. Annexstein, "Generating de Bruijn sequences: an efficient implementation," *IEEE Trans. Computers*, vol. 46, no. 2, pp. 198-200, Feb. 1997.

[2] N. G. de Bruijn, "A combinatorial problem," *Proc. Kon. Ned. Akad. Wetensch*, vol. 49, pp. 758-764, 1946.

[3] T. Etzion and A. Lempel, "Algorithms for the generation of full-length shift-register sequences," *IEEE Trans. Inf. Theory*, vol. 30, no. 3, pp. 480-484, May 1984.

[4] H. Fredricksen, "A class of nonlinear de Bruijn cycles," *J. Comb. Theory*, Ser. A, vol. 19, no. 2, pp. 192-199, Sep. 1975.

[5] H. Fredricksen, "A survey of full length nonlinear shift register cycle algorithms," *SIAM Rev.*, vol. 24, no. 2, pp. 195-221, Apr. 1982.

[6] S. W. Golomb, *Shift Register Sequences*, San Francisco, CA: Holden-Day, 1967.

[7] S. W. Golomb and G. Gong, *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*, Cambridge University Press, New York, NY, 2005.

[8] E. R. Hauge and T. Helleseth, "De Bruijn sequences, irreducible codes and cyclotomy," *Discrete Math.*, vol. 159, no. 1, pp. 143-154, Nov. 1996.

[9] E. R. Hauge and J. Mykkeltveit, "On the classification of deBruijn sequences," *Discrete Math.*, vol. 148, no. 1, pp. 65-83, Jan. 1996.

[10] F. Hemmati, "A large class of nonlinear shift register sequences," *IEEE Trans. Inf. Theory*, vol. 28, no. 2, pp. 355-359, Mar. 1982.

[11] C. J. A. Jansen, W. G. Franx and D. E. Boekee, "An efficient algorithm for the generation of deBruijn cycles," *IEEE Trans. Inf. Theory*, vol. 37, no. 5, pp. 1475-1478, Sep. 1991.

[12] A. Lempel, "On a homomorphism of the de Bruijn graph and its applications to the design of feedback shift registers," *IEEE Trans. Computers*, vol. 19, no. 12, pp. 1204-1209, Dec. 1970.

[13] C.Y. Li, X.Y. Zeng, T. Helleseth, C.L. Li and L. Hu, "The properties of a class of linear FSRs and their applications to the construction of nonlinear FSRs," *IEEE Trans. Inf. Theory*, vol. 60, no. 5, pp. 3052-3061, May 2014.

[14] C. Y. Li, X.Y. Zeng, C. L. Li and T. Helleseth, "A class of de Bruijn sequences," *IEEE Trans. Inf. Theory*, vol. 60, no. 12, pp. 7955-7969, Dec. 2014.

[15] C. Y. Li, X.Y. Zeng, C. L. Li, T. Helleseth, and M. Li, "Construction of de Bruijn sequences from LFSRs with reducible characteristic polynomials," IEEE Trans. Inf. Theory, vol. 62, no. 1, pp. 610-624, Jan. 2016.

[16] M. Li, Y. P. Jiang, and D. D. Lin, "The adjacency graphs of some feedback shift registers," Designs, Codes, Cryptogr., DOI: 10.1007/s10623-016-0187-6.

[17] M. Li, D. D. Lin, "The adjacency graphs of linear feedback shift registers with primitive-like characteristic polynomials," Cryptology ePrint Archive, 2016/269. www.iacr.org

[18] K. B. Magleby, "The synthesis of nonlinear feedback shift registers," Tech. Rep. 6207-1, Stanford Electronic Labs, Stanford, CA, 1963.

[19] J. Mykkeltveit, M. K. Siu and P. Tong, "On the cycle structure of some nonlinear shift register sequences," *Inf. Contr.*, vol. 43, no. 2, pp. 202-215, Nov. 1979.

[20] J. Mykkeltveit and J. Szmidt, "On cross joining de Bruijn sequences," Contemporary Mathematics, vol. 632, pp. 333-344, 2015.

[21] N. Zierler, "Linear recurring sequences," *J. Soc. Indust. Appl. Math.*, vol. 7, no. 1, pp. 31-48, Mar. 1959.